## REMARKS

Claims 1-74 remain pending in this application. Claims 1-74 have been rejected. Applicants cancel claims 1 and 70-74 without prejudice.

Claim 2 has been amended to read, "wherein said secure cryptographic system is remote from said user and said user is connected to the system via a communication link." Support for this amendment is found throughout the specification, e.g. at page 4, lines 22-24.

Claims 10, 14, 36, 37, 45, 46, 54, and 59 have been amended to include the terminology, "wherein said user is connected to said remote secure server via communication link." Support for this amendment is found throughout the specification, e.g., at page 15, lines 22-24.

Claim 10 has been amended to read, "...associating a user from multiple users with one or more keys from a plurality of private cryptographic keys generated and stored on a remote secure server...." Support for this amendment is in the specification at page 13, lines 26-27.

Claim 10 has been amended to read, "...comparing, exclusively on said remote secure server, said authentication data received from said user to authentication data stored on said remote secure server corresponding to said user, thereby verifying the identity of said user...." Support for this amendment is in the specification at page 3, lines 18-21.

Claim 14 has been amended to include the terminology, "...wherein said trust engine comprises of an authentication system..." Support for this amendment is in the specification at page 6, line 4.

Claim 30 has been amended to read, "...user is remote from said cryptographic system and is connected to it via a communication link." Support for this amendment is in the specification at page 10, lines 20-22.

Claim 30 has been amended to read, "...a data assembling module remote from said user which processes the substantially randomized data portions from at least two of said data storage facilities to assemble said at least one private cryptographic key from said plurality of private cryptographic keys..." Support for this amendment is in the specification at page 6, lines 22-26.

Claim 36, 37, and 45 have been amended to include the terminology, "...splitting authentication data into two or more portions with a data splitting module

remote from said user....". Support for this amendment is in the specification at page 6, lines 22-26.

Claim 36 has been amended to read, "...combining at said remote trust engine an authentication data portion with a first substantially random value to form a first combined value; combining a second authentication data portion with a second substantially random value to form a second combined value...." Support for this amendment is in the specification at page 6, lines 17-20 and p age 7, lines 18-20.

Claims 36 and 45 have been amended to include the terminology, "...wherein said trust engine comprises multiple remote data storage facilities...." Support for this amendment is in the specification at page 6, lines 4-8.

Claims 37, 45, and 46 have been amended to read, "...generating private cryptographic keys within a remote trust engine...." Support for this amendment is in the specification at page 13, lines 26-27.

Claims 37 and 46 have been amended to include the following language, "...wherein said remote trust engine comprises multiple computer accessible storage media...." Support for this amendment is in the specification at page 13, lines 26-27.

Claim 46 has been amended to read, "...combining said cryptographic key portions with a first set of bits to form a second set of bits; combining said cryptographic key portions with a third set of bits to form a fourth set of bits...." Support for this amendment is in the specification at page 6, lines 17-20 and p age 7, lines 18-20.

Claim 54 has been amended to read, "...receiving in a remote data assembling module, a substantially randomized sensitive data portion from a first computer accessible storage medium remote from said users; receiving in said data assembling module, a second substantially randomized data portion from a second computer accessible storage medium remote from both the user and the first computer accessible storage medium, processing said substantially randomized sensitive data and said substantially randomized data in said data assembling module to assemble said sensitive data...." Support for this amendment is in the specification at page 6, lines 10-16.

Claim 54 has been amended to include the following language, "...wherein said trust engine comprises said data assembling module and a software engine..." Support for this amendment is in the specification at page 43, lines 22-24.

Claim 59 has been amended to read, "...wherein said authentication engine contains a data assembling module assembles substantially randomized enrollment authentication data portions, from various data storage facilities, to form the enrollment authentication data...." Support for this amendment is in the specification at page 6, lines 10-16.

Claim 59 has been amended to include the terminology, "wherein the secure authentication system is part of said remote trust engine...." Support for this amendment is in the specification at page 6, lines 4-5.

Claim 65 has been amended to read, "...a plurality of enrollment authentication data corresponding to multiple users..." Support for this amendment is in the specification at pages 4-5, lines 30 and 1-2.

Claim 65 has been amended to read, "...wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives authentication data from a user and forwards a request for the data assembling module to assemble said enrollment authentication data from substantially randomized data portions, and wherein said authentication engine compares said authentication data from user and enrollment authentication data assembled from said first and second depositories, and determines an authentication result,...." Support for this amendment is in the specification at page 6, lines 10-16.

Claim 65 has been amended to include the terminology, "...wherein said first and second trust engines are remote from said user and said user is connected to said trust engines via a communication link." Support for this amendment is in the specification at page 15 lines 22-24 and page 49, lines 27-30.

No new matter has been added by these amendments and these amendments are made only to more clearly define the claimed inventions and are not made in response to any rejection of the claims. By these amendments, Applicants do not acquiesce to the propriety of any of the Examiner's rejections and do not disclaim any subject matter to which the Applicants are entitled. *Warner-Jenkinson Co. v. Hilton-Davis Chem. Co.*, 41 U.S.P.Q.2d 1865 (U.S. 1997).

## I. REJECTION OF CLAIMS 10-53 UNDER 35 U.S.C. § 102(e) AS BEING ANTICIPATED BY EPSTEIN (US 6,453,416)

The Examiner rejected claims 10-53 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,453,416, issued to Epstein ("*Epstein*"). Office

Action of April 24, 2006, page 3. Applicants respectfully traverse.

In order to support an anticipation rejection under 35 U.S.C. § 102, the Examiner must illustrate that each and every element of a claimed invention was disclosed within a single prior art reference. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). A claimed invention is anticipated only when it is "known to the art in the detail of the claim." *Karsten Manufacturing Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). In other words, not only must the limitations of the claim be shown in a single prior art reference, the limitations must be "arranged as in the claim." *Id.*

The present invention, in light of the amendments to independent claims 10, 14, 30, 36, 37, 45, and 46 is not anticipated by *Epstein*. Specifically, *Epstein* does not anticipate claims 10-53 because it does not disclose each and every element of those claims. *Epstein* does not anticipate amended claim 10 because it does not teach the method of facilitating cryptographic functions on a remote secure server. See *Epstein* at column 7, lines 37-48.

Applicants have amended independent claim 10 to clarify that the private keys are stored on the secure server, not on "a smartcard associated with the user's machine" as *Epstein* relates. The amended claim also recites that the user is remote from the server and connects to the remote secure server via a communication link. Amended claim 10 now recites in relevant part:

> A method of facilitating cryptographic functions, said method comprising:
> associating a user from multiple users with one or more keys from a plurality of private cryptographic keys ***generated*** and stored on a ***remote*** secure server;
> ...
> ***wherein said user is connected to said remote secure server via a communication link.***

(Emphasis added.) *Epstein* does not anticipate the present invention as the present invention stores all user information on a remote secure server.

Furthermore, amended claim 10 clarifies that the present invention generates the private keys within the trust engine. Amended claim 10 now recites in relevant part:

> A method of facilitating cryptographic functions, said method comprising:

> associating a user from multiple users with one or more keys from a plurality of private cryptographic keys ***generated*** and stored on a ***remote*** secure server;
> ...

(Emphasis added.) The specification defines a trust engine as synonymous with a secure server. See Specification at page 3, lines 15-18. Thus, unlike in *Epstein* where the private key is stored on the user's smartcard located on the user's equipment and is accessible by the user, the private key of the present invention is generated within the trust engine and is not accessible by the user. Id. Storing the private keys on a remote secure server as opposed to the user's equipment increases security, portability, and availability. Specification at page 10, lines 25-26. In addition, the user's smartcard may be stolen, broken, lost, or compromised when connected to the internet.

Applicants have also amended claim 10 to clarify that the authentication occurs exclusively on the secure server which is remote from the user. Amended claim 10 now recites in relevant part:

> A method of facilitating cryptographic functions, said method comprising:
> ...
> comparing, ***exclusively on said remote secure server***, said authentication data ***received from said user*** to authentication data ***stored on said remote secure server*** corresponding to said user, thereby verifying the identity of said user".
> ...
> ***wherein said user is remote from the remote secure server and is connected to the server via a communication link.***

(Emphasis added.)

*Epstein* relates to storing the user's private key on the user's smartcard. *Epstein* at columns 5, line 63 to column 6, line 6. *Epstein* relates that the smartcard "has previously been loaded in a secure manner during a setup phase when the smartcard was issued with a generated private key assigned to the user". Id. The smartcard is located on the user's equipment and communicates with the server:

> Further, **a smartcard reader associated with user equipment** is configured for coupling to the user's smartcard for communication therewith, and **is controlled by a background process or back end of the user equipment which also routes communication to and from smartcard to network, and ultimately server, via link.**

(Emphasis added.) *Epstein* at column 4, line 64 to column 5, line 3; see also FIG. 1.

Thus, the smartcard is not located on a remote server. Id. Consequently, the private keys that are stored on the smartcard are not on the server.

*Epstein* relates to authentication which occurs both on the user's smartcard and the server. *Epstein* at column 4, line 64 to column 5, line 3; column 6, lines 28-38. The first part of authentication takes place on the user's smartcard.

> Since this insecure route exposes the communication to and from smartcard to being recorded and replayed by a malicious person monitoring the network, security measures are taken including the provision of a random number generator and **an authentication means in the smartcard**

(Emphasis added.) *Epstein* at column 4, line 64 to column 5, line 3. The smartcard, as indicated above, is located on the user's machine which is remote from the server. See supra pp. 20-21. Once the smartcard produces an authentication result the smartcard generates a digital signature (DS), which the server then authenticates. *Epstein* column 6, lines 28-30. Authentication later takes place on the server.

> **Server comprises an authentication means**, including, as is typical for authenticating the digital signature DS received from smartcard

(Emphasis added.) Id. Epstein relates to producing a verified DS only when the smartcard and the server have completed their respective authentication processes. *Epstein* at column 7, lines 52-65. Thus, *Epstein* does not relate to an authentication process which occurs solely on the server.

Unlike *Epstein*, which discusses an authentication process which takes on both the user's smartcard and the server, the present invention defines an authentication process which occurs exclusively on a remote secure server. *Epstein* admits that communication to and from the smartcard, like that which occurs during authentication, is "insecure" and is exposed to "being recorded and replayed by a malicious person". *Epstein* columns 4 and 5, lines 64-67 and 1-3. This insecure route between the smartcard and the server is eliminated in the present invention because all authentication processes occur on the remote secure server.

Therefore, *Epstein* does not anticipate claim 10 because it does not teach or disclose the limitations on the location of the private keys or the location of the authentication process. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 10 and its dependent claims 11-13.

Examiner rejected claims 14-29 under 35 U.S.C. 102(e) as being anticipated

by *Epstein*. However, the Examiner did not provide any reasoning for this rejection. According to the MPEP, an Examiner must "[designate] as nearly as practicable" the part relied upon "when a reference is complex or shows or describes inventions other than that claimed by the applicant." MPEP, §707(c)(2). Furthermore, "the pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified." Id. Because Examiner has not provided an explanation for the rejection of claims 14-29 under 35 U.S.C. §102(e). Applicants request withdrawal of the present rejection. To expedite prosecution, however, Applicants have assumed that Examiner maintains the same explanation for the rejection as provided in the previous office action filed on September 16, 2005, and provide the following traversal or the rejection.

Applicants have amended independent claim 14 to clarify that the enrollment authentication data is stored on the authentication system in substantially randomized data portions. Amended claim 14 now recites in relevant part:

> An authentication system for uniquely identifying a user through secure storage of said user's enrollment authentication data, said authentication system comprising:
>
> a plurality of data storage facilities, wherein each data storage facility ***is remote from said user and*** includes a computer accessible storage medium which stores one of substantially randomized data portions of ~~***at least one piece of enrollment authorization data from***~~ enrollment authentication data; and

(Emphasis added.) Applicants have also amended claim 14 to further clarify that the authentication system which stores the enrollment authentication data is remote from the user. Amended claim 14 now recites in relevant part:

> ...
> ***wherein said trust engine is comprises an authentication system,***
>
> ***wherein said trust engine is remote from said user and said user is connected to said trust engine via a communication link.***

(Emphasis added.) *Epstein* relates to comparing user input data to user identifying data in order to authenticate the user. *Epstein* at column 6, lines 12-19. Thus user identifying data is the equivalent of authentication data. *Epstein* also discusses storing the user identifying data in its whole form, not in portions. *Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. The user identifying data is previously

> ...loaded in a secure manner during a setup phase when the smartcard

> [is] issued...with the user's identifying data U derived from information entered by the user.

Id.

> *Epstein* relates to storing the user identifying data on the user's smartcard.
>
> **Smartcard also includes a memory for storing** at least the most recently generated random number RN, and the user's private key and **user identifying data**...

(Emphasis added.) *Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. As indicated earlier, in *Epstein* the user's smartcard is located in the user's equipment remote from the server. See supra pp. 20-21. Thus, the user identifying data is stored in its whole form on the user's machine not on a remote secure server.

*Epstein* does not anticipate claim 14 of the present invention because *Epstein* relates to storing the user identifying data in its whole form on the user's machine. In contrast, the present invention defines storing the enrollment authentication data in the form of substantially randomized portions on a server remote from the user. Therefore *Epstein* does not anticipate the present invention. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 14 and dependent claims 15-29.

Applicants have amended independent claim 30 to clarify that the private cryptographic keys are divided into portions and then stored on a plurality of data storage facilities remote from the user. Amended claim 30 now recites in relevant part:

> ...
> a plurality of data storage facilities ***remote from a user***, wherein each data storage facility includes a computer accessible storage medium which stores ~~***one of***~~ substantially randomized data portions of at least one ***private*** cryptographic key[[s]] from a plurality of ***private*** cryptographic keys; and
> ...
>
> ***Wherein said user is remote from said cryptographic system and is connected to it via a communication link***

(Emphasis added.) *Epstein* does not anticipate amended claim 30 because unlike *Epstein* which only relates to storing the public keys on the server, the present invention defines storing the private keys on a remote secure server or cryptographic system.

Applicants have amended claim 30 to clarify that the data splitting module and data assembling modules perform their functions on private keys. Amended claim 30 now recites in relevant part:

> a cryptographic engine ***remote from said user*** which communicates with said plurality of data storage facilities and comprises:
>
> a data splitting module ***remote from said user*** which operates on said ***private*** cryptographic keys to create said substantially randomized data portions of at least one ***private*** cryptographic key,
>
> a data assembling module ***remote from said user*** which processes the substantially randomized data portions from at least two of said data storage facilities to assemble said at least one ***private*** cryptographic key from said plurality of ***private*** cryptographic keys, and
> ...

(Emphasis added.) Storing the private key in portions as opposed to in its whole form increases the security of the system. Specification at page 29, lines 15-18.

> As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions **increases security and provides for maintained trust in the data even if one of the data storage facilities...is compromised.**

(Emphasis added.) Id.

*Epstein* relates to storing the undivided private key on the user's smartcard. *Epstein* at Column 1, lines 35-37; see also FIG. 1. As indicated earlier, the user's smartcard is located in the user's equipment remote from the server. See supra pp. 20-21. Instead, *Epstein* discusses storing the private key in its whole form on the user's machine. Furthermore, *Epstein* relates that the public keys, not the private keys, are stored in the memory of the server. *Esptein* at Column 6, Lines 39-49.

> Server comprises a memory which may be or include RAM, ROM, a hard disk, or other memory or media. **Memory contains respective sections, or fields in a data structure, for storing user IDs, public keys, documents and associated digital signatures DS, respectively, for all users,** which are indexed or otherwise addressable or retrievable by ID, and also a section for storing one or more applets.

(Emphasis added.) See supra pp. 20-21. *Epstein* at column 6, lines 39-46. *Epstein* relates to storing the public keys on the server and the private keys on the user's smartcard which is remote from the server. Id.; See supra pp. 20-21.

*Epstein* does not anticipate the present invention because unlike *Epstein* the

present invention stores the private keys on a remote secure server not a smartcard on the user's machines. In addition, *Epstein* does not anticipate the present invention because *Epstein* relates to storing the key as a whole, whereas the present invention defines storing the private key in substantially randomized portions. Indeed, *Epstein* does not teach either a data splitting module or a data assembling module because these components are not necessary when the private keys are stored in their whole form. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 30 and dependent claims 31-35.

Applicants have amended independent claim 36 to clarify that the system splits the authentication data into portions and combines these portions with random values. Claim 36 recites in relevant part:

> ...
> receiving authentication data ***from a user*** at a trust engine ***remote from said user***;
>
> ***splitting authentication data into at least two portions with a data splitting module remote from said user;***
> ...

(Emphasis added.) Applicants have also amended claim 36 to explain that these authentication data portions are combined with random values. Amended claim 36 recites in relevant part:

> ...
> combining at said ***remote*** trust engine ~~***said***~~ ***an*** authentication data ***portion*** with a first substantially random value to form a first combined value;
>
> combining ~~***said***~~ ***a second*** authentication data ***portion*** with a second substantially random value to form a second combined value;
>
> creating a first pairing of said first substantially random value with said second combined value;
>
> creating a second pairing of said first substantially random value with said second substantially random value;
> ...

(Emphasis added.) Applicants have also amended claim 36 to clarify that the pairings of the random values and the authentication data portions and the random values themselves are stored in multiple remote data storage facilities.

...

> storing said first pairing in a first secure data storage facility ***located on a server remote from said user***; and
>
> storing said second pairing in a second secure data storage facility remote from ***said user and*** said first secure data storage facility;
>
> ***wherein the trust engine comprises multiple remote data storage facilities; and***
>
> ***wherein said user is remote from said trust engine and is connected to it via a communication link.***

(Emphasis added.) Storing the authentication data remotely, like storing the private keys remotely, increases the security of the system. See supra p. 20; specification at p. 6, lines 27-28. Storing the authentication data in portions in multiple remote data storage facilities protects "the authentication data against compromise [sic.] of any individual data storage facility". Specification at p. 6, lines 27-28.

*Epstein* relates to storing the user identifying data (U) on the user's smartcard.

> **Smartcard also includes a memory for storing** at least the most recently generated random number RN, and the user's private key and **user identifying data U**...

(Emphasis added.) *Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. As indicated above, the user's smartcard is located in the user's equipment remote from the server. See supra pp. 20-21. *Epstein* discusses storing the user identifying data in its whole form, not in portions. *Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. The user identifying data is previously

> ...loaded in a secure manner during a setup phase when the smartcard [is] issued...with the user's identifying data U derived from information entered by the user.

Id. *Epstein* later relates comparing user input data to user identifying data in order to authenticate the user, thus revealing that user identifying data is the equivalent of authentication data. *Epstein* at column 6, lines 12-19.

*Epstein* does not anticipate the present invention because it does not teach: splitting the user identifying data, the equivalent of authentication data, into portions; combining these authentication data portions with random values; or storing these combined values on multiple remote data store facilities. *Epstein* relates to storing the authentication data in its whole form on the user's smartcard whereas the present

invention defines splitting the authentication data first into portions, combining these portions with random values, and storing the combined values in multiple remote data storage facilities. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 36.

Applicants have amended claim 37 to clarify that the system first splits the authentication data into at least two portions. Amended independent claim 37 recites in relevant part:

> A method of storing authentication data comprising:
>
> ~~receiving~~ ***generating private*** cryptographic ~~data~~ ***keys within a remote trust engine***;
>
> ***splitting authentication data into at least two portions with a data splitting module remote from said user;***

(Emphasis added.) Applicants have also amended claim 37 to clarify that the authentication data portions are combined with a set of bits to form another set of bits. Amended claim 37 recites in relevant part:

> ...
> combining ~~***said***~~ ***a first*** authentication data ***portion*** with a first set of bits to form a second set of bits;
>
> combining ~~***said***~~ ***a second*** authentication data ***portion*** with a third set of bits to form a fourth set of bits;
>
> creating a first pairing of said first set of bits with said third set of bits; creating a second pairing of said first set of bits with said fourth set of bits;
> ...

(Emphasis added.) In addition, applicants have amended the claim to explain that these sets of bits are stored in remotely accessible medium in separate computers. Amended claim 37 recites in relevant part:

> ...
> storing one of said first and second pairings in a first computer accessible storage medium ***remote from said user***; and
>
> storing the other of said first and second pairings in a second computer accessible storage medium ***remote from both said user and said first computer accessible storage medium,***

> ***wherein said trust engine comprises multiple computer accessible storage media; and***
>
> ***wherein the user is remote from said trust engine and is connected to it via a communication link.***

(Emphasis added.) As mentioned in the discussion of claim 36 above, *Epstein* relates to storing the user identifying data in its whole form, whereas the present invention defines storing the authentication data in portions combined with bits. Furthermore, *Epstein* relates to storing the user identifying data on the user's smartcard. In contrast, the present invention defines storing the authentication data portions combined with bits and the bits themselves in multiple remote data storage facilities. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 37 and dependent claims 38-44.

Applicants have amended independent claim 45 to clarify that the trust engine first generates the private cryptographic keys. Amended claim 45 recites in relevant part:

> A method of storing ***portions of private*** cryptographic ~~***data***~~ ***keys*** in geographically remote secure data storage facilities thereby protecting said cryptographic data against compromise of any individual data storage facility, said method comprising:
>
> ~~receiving~~ ***generating private*** cryptographic ~~data~~ ***keys*** at a ***remote*** trust engine;
>
> ...

(Emphasis added.) Applicants have also amended the claim to clarify that the data splitting module splits each key into at least two portions. Amended claim 45 recites in relevant part:

> ...
> ***splitting each private cryptographic key into at least two portions with a data splitting module remote from a user;***
> ...

(Emphasis added.) In addition, Applicants have amended claim 45 to clarify that these cryptographic key portions combined with random values and the random values themselves are stored in separate secure data storage facilities which are remote from the user. Amended claim 45 recites in relevant part:

> ...
> storing said first pairing in a first secure data storage facility ***located on a server remote from said user***; and

storing said second pairing in a secure second data storage facility remote from ***both said user and*** said first secure data storage facility,

***wherein said trust engine comprises multiple remote data storage facilities; and***

***wherein said user is remote from said trust engine and is connected to it via a communication link.***

(Emphasis added.)

*Epstein* relates to storing the user's private key on the user's smartcard. See supra pp. 20-21. As indicated above, in *Epstein* the user's smartcard is loaded during the setup phase with a "generated private key assigned to the user". Id. The user's smartcard is located in the user's equipment remote from the server. Id. *Epstein* does not teach

storing substantially randomized key portions in multiple data storage facilities. See supra p. 23.

*Epstein* relates to loading the user's private key onto a smartcard during the setup phase, whereas the present invention defines generating the private key within the trust engine. In addition, unlike *Epstein* which discusses storing the private key on the user's smartcard remote from the server, the present invention defines storing the private key in portions in multiple remote data storage facilities. Furthermore, *Epstein* relates to storing the private key in its whole form, whereas the present invention defines dividing the private key into key portions which are then combined with random values. *Epstein* does not teach splitting the private key into portions, combining these portions with random values, or storing these combined and random values in multiple remote data storage facilities. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 45.

Applicants have amended claim 46 to clarify that the trust engine first generates the private cryptographic keys. Amended claim 46 recites in relevant part:

A method of storing cryptographic data comprising:

~~receiving~~ ***generating private*** cryptographic ~~data~~ ***keys within a remote trust engine***;

(Emphasis added.) Applicants have also amended the claim to clarify that the data splitting module splits each key into at least two portions. Amended independent claim 46 recites in relevant part:

...

***splitting each private cryptographic key into at least two portions with a data splitting module remote from a user;***

(Emphasis added.) In addition, Applicants have amended claim 46 to clarify that these cryptographic key portions combined with bits and the bits themselves are stored in separate secure data storage facilities which are remote from the user. Amended claim 46 recites in relevant part:

> storing one of said first and second pairings in a first computer accessible storage medium ***remote from said user***; and
>
> storing the other of said first and second pairings in a second computer accessible storage medium ***remote from both said user and said first computer accessible storage medium,***
>
> ***wherein said trust engine comprises multiple computer accessible storage media; and***
>
> ***wherein said user is remote from said trust engine and is connected to it via a communication link.***

(Emphasis added.) *Epstein* relates to storing the user's private key on the user's smartcard. See supra pp. 20-21. As indicated above, the user's smartcard is loaded during the setup phase with a "generated private key assigned to the user". Id. The user's smartcard is located in the user's equipment remote from the server. Id. Thus, the user's private keys are located in the user's equipment, not on a remote secure server. Indeed, *Epstein* does not mention storing substantially randomized key portions in multiple data storage facilities. See supra p. 23.

*Epstein* does not anticipate the present invention because *Epstein* only relates to loading the user's private key onto a smartcard during the setup phase, whereas the present invention defines generating the private key within the trust engine. In addition, unlike *Epstein* which requires storing the private key on the user's smartcard remote from the server, the present invention defines storing the private key in the form of portions in multiple computer accessible storage media. Furthermore, *Epstein* relates to storing the private key in its whole form, whereas the present invention defines dividing the private key into key portions which are then combined with bits. *Epstein* does not teach splitting the private key into portions, combining these portions with bits, or storing these combinations and bits in multiple computer accessible storage media. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 46 and dependent claims 47-

53.

## II. REJECTION OF CLAIMS 54-58 and 70-74 UNDER 35 U.S.C. § 102(e) AS BEING ANTICIPATED BY BORZA (US 5,995,630)

The Examiner rejected claims 54-58 and 70-74 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,995,630, issued to Borza ("*Borza*"). Office Action of April 24, 2006, page 11. Applicants respectfully traverse.

In order to support an anticipation rejection under 35 U.S.C. § 102, the Examiner must illustrate that each and every element of a claimed invention was disclosed within a single prior art reference. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). A claimed invention is anticipated only when it is "known to the art in the detail of the claim." *Karsten Manufacturing Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). In other words, not only must the limitations of the claim be shown in a single prior art reference, the limitations must be "arranged as in the claim." Id. The present invention, in light of the amendments to independent claim 54, is not anticipated by *Borza*.

Applicants have amended claim 54 to clarify that sensitive data, such as a private key, is stored in at least two substantially randomized portions in remote computer accessible storage media. Applicants have also amended claim 54 to explain that a data assembling module remote from the user receives and assembles these substantially randomized sensitive data portions to form the sensitive data. Amended claim 54 recites in relevant part:

> A method of handling sensitive data from a plurality of users in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:
>
> receiving in a ~~***software module***~~ ***remote data assembling module, a*** substantially randomized sensitive data ***portion*** from a first computer accessible storage medium ***remote from said users***;
>
> receiving in said ~~***software module***~~ ***data assembling module, a second*** substantially randomized data ***portion*** from ***a*** second computer accessible storage medium ***remote from both said users and said first computer accessible storage medium***,
>
> processing said substantially randomized sensitive data and said substantially randomized data in said ~~***software module***~~ ***data assembling module*** to assemble said sensitive data; and

...

(Emphasis added.) In addition, Applicants have amended claim 54 to clarify that the data assembling module and the software engine are located on the trust engine which is remote from the user. The amendment also explains that the user is connected to the trust engine via communication link. Finally, the amendment clarifies that authentication takes place on the trust engine which is remote from the user's machine. Amended claim 54 recites in relevant part:

> ...
> employing said sensitive data in a software engine, ***on a remote trust engine comprising an authentication and cryptographic engines***, to authenticate exactly one of said plurality of users,
>
> ***wherein said trust engine comprises said data assembling module and a software engine; and***
>
> ***wherein said users are remote from the trust engine and are connected to it via a communication link.***

(Emphasis added.) Performing the authentication on the server allows the user to perform cryptographic functions while the user does not have access to her home machine. Specification at page 14, lines 2-5.

> **Such remote access advantageously allows users to remain completely mobile** and access cryptographic functionality through practically any Internet connection, such as cellular and satellite phones, kiosks, laptops, hotel rooms and the like.

(Emphasis added.) Id.

*Borza* discusses a "key for use in encryption and/or decryption". *Borza* at column 8, lines 31-37. The key is stored on a personal computer. *Borza* at column 8, lines 31-37.

> The computer also has, stored in non-volatile memory, a key for use with encryption or decryption.

Id. *Borza* does not discuss teach storing the keys on a server. Indeed, *Borza*'s system does not contain a server.

*Borza* also relates to "data selected or calculated in dependence upon biometric information" from the user which is "encoded within an image frame." *Borza* at column 6, lines 49-51. *Borza* also states that,

> the advantage to encoding the user's biometric information within an image frame is that the **imaging system need only provide data in the form of a portion of an encryption key or a key reference and the biometric data in the form of an image; the computer then processes the image to determine another portion of the key or of the key identifier.**

(Emphasis added.) *Borza* at Column 6, lines 61-66 (emphasis). Thus, *Borza* relates to the assembly of the key from its portions occurring on the user's computer, not on a remote server.

*Borza* relates to an authentication process which "compares the data with the biometric data previously stored in non-volatile memory." *Borza* at column 9, lines 26-28. This authentication process takes place on the user's computer. Id. Thus, *Borza* does not teach authentication which occurs on the server.

*Borza* does not anticipate the current invention. Unlike *Borza* which relates to storing keys or key portions on the user's computer, the present invention defines storing sensitive data, such as keys, in substantially randomized data portions on a server remote from the user. In addition, *Borza* relates to reconstructing the keys from their portions on the user's computer, whereas the present invention defines reconstructing the sensitive data from its portions on the trust engine which is remote from the user. Lastly, *Borza* relates to authentication which takes place on the user's computer. By contrast, the current invention defines authentication which occurs on a trust engine remote from the user. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 54 and dependent claims 55-58.

In order to aid prosecution and allowance, Applicants hereby cancel independent claim 70 and dependent claims 71-74 without prejudice. By this cancellation, Applicants do not acquiesce to the propriety of the Examiner's rejection.

## III. REJECTION OF CLAIMS 1-9 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER BORZA (US 5,995,630), AND FURTHER IN VIEW OF EPSTEIN (US 6,453,416)

The Examiner rejected claims 1-9 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,995,630, issued to *Borza*, and in further view of U.S. Patent No. 6,453,416, issued to *Epstein*. Office Action of April 24, 2006, page

14. Applicants respectfully traverse.

To maintain a proper rejection under 35 U.S.C. §103, the Examiner must meet four conditions to establish a *prima facie* case of obviousness. First, the Examiner must show that the prior art suggested to those of ordinary skill in the art that they should make the claimed composition or device or carry out the claimed process. Second, the Examiner must show that the prior art would have provided one of ordinary skill in the art with a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be adequately founded in the prior art and not in an applicant's disclosure. Third, the prior art must teach or suggest all the claim limitations. *In re Vaeck*, 20 U.S.P.Q.2d 1438, 1442 (Fed. Cir. 1991). Fourth, if an obviousness rejection is based on some combination of prior art references, the Examiner must show the suggestion, teaching, or motivation to combine the prior art references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

In order to aid prosecution and allowance, Applicants hereby cancel claim 1 without prejudice. By this cancellation, Applicants do not acquiesce to the propriety of the Examiner's rejection.

Applicants have amended claim 2 to clarify that the private keys are stored on a depository system which is remote from the user. Amended claim 2 now recites in relevant part:

> A secure cryptographic system, comprising:
>
> a depository system, ***remote from a user***, having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;
> ...

(Emphasis added). In addition, Applicants have amended claim 2 to further clarify that the user is remote from the trust engine, which contains the depository system, and connected to the trust engine via a communication link. Amended claim 2 now recites in relevant part:

> ...
> wherein said secure cryptographic system is ~~***remotely accessible***~~ ***remote from said user and said user is connected to the system via a communication link.***

(Emphasis added). Lastly, Applicants have amended claim 2 to clarify that the authentication engine performs the entire authentication process and produces the final authentication result. Amended claim 2 now recites in relevant part:

> ...
> an authentication engine, ***remote from said user***, which compares authentication data received ~~***by***~~ ***from*** one of said multiple users to enrollment authentication data corresponding to said one of multiple users and received from said depository system, thereby producing ~~***an***~~ ***the final*** authentication result;
> ...

(Emphasis added).

Examiner indicates that "Borza teaches encryption techniques to provide security for computer communications and files for computers and networks." Office Action of April 24, 2006, page 18. Examiner then states that, "Borza did not clearly point out that the secure cryptographic system is remotely accessible." Id. Examiner then explains that:

> *Epstein* teaches a method of facilitating cryptographic [sic] comprising associating a user from multiple users with one or more keys from a **plurality of private cryptographic keys stored on a secure server,** receiving authentication data from the user; and comparing the authentication data to authentication data corresponding to the user; thereby verifying the identity of the user; and wherein utilizing the one or more keys to perform cryptographic functions without releasing the one or more keys to the user.

(Emphasis added). Id. at page 16. As indicated earlier, *Epstein* does not teach or suggest "storing a plurality of private cryptographic keys stored on a secure server." Id., See supra pp. 20-21. Instead, *Epstein* discusses storing the private keys on the user's smartcard which is not on the remote server. See supra pp. 20-21. Furthermore, the Examiner claims that *Epstein* relates to not releasing "the one or more keys to the user." Office Action of April 24, 2006, page 16. This is not the case given that the private keys are stored on the user's machine to which the user presumably has access.

Examiner quotes the field of the invention from *Epstein*:

> The present invention relates to secure proxy signing devices for forming and supplying digital signatures over a network on behalf of users so that private keys are never extant at user equipment which is not secure, and to methods of using, and systems employing, such devices.

Office Action of April 24, 2006, page 16; *Epstein* at column 1, Lines 6-10. Indeed, the private keys are "extant at user equipment" as the keys are stored on the user's smartcard which is part of the user's machine. Id.; *Epstein* at columns 4 and 5, lines 64-67 and 1-3; See also FIG. 1. Furthermore, storing private key(s) on the user's smartcard may expose the private key to compromise if the smartcard itself is stolen, lost, or connected insecurely to the Internet. Specification at page 3, lines 3-11.

As the Examiner correctly indicates, *Epstein* does discuss a server which "comprises an authentication means." Office Action of April 24, 2006, page 15; *Epstein* at column 6, line 28. However, as indicated earlier, *Epstein* does not teach or suggest authentication which occurs solely on the server. See supra p. 23. *Epstein* only relates to an authentication process which occurs in part on the user's smartcard and in part on the server. Id.

*Borza*, in further view of *Epstein*, does not render the present invention unpatentable. The prior art does not teach or suggest all the claim limitations. Id. As the Examiner indicated, *Borza* alone does not "clearly point out that the secure cryptographic system is remotely accessible." However, counter to the Examiner's assertions, *Epstein* does not teach or suggest "associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure server." (Emphasis added.) Office Action of April 24, 2006, page 16. As indicated earlier, *Epstein* relates to storing the private keys on the user's smartcard which is remote from the server. See supra pp. 20-21. Moreover, unlike the present invention, *Epstein* does not discuss an authentication process which occurs solely on the server. See supra p. 22. *Borza* does not cure this significant deficiency of *Epstein*.

*Borza* in view of *Epstein* does not teach or suggest to one of ordinary skill in the art storing the private keys on a secure server or authentication which occurs solely on the server. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 2 and dependent claims 3-9.

## IV. REJECTION OF CLAIMS 14-29 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER EPSTEIN (US 6,453,416), AND FURTHER IN VIEW OF BORZA (US 5,995,630)

The Examiner rejected claims 14-29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,453,416, issued to *Epstein*, and in further view of

U.S. Patent No. 5,995,630, issued to *Borza*. Office Action of April 24, 2006, page 20. Applicants respectfully traverse.

To maintain a proper rejection under 35 U.S.C. §103, the Examiner must meet four conditions to establish a *prima facie* case of obviousness. First, the Examiner must show that the prior art suggested to those of ordinary skill in the art that they should make the claimed composition or device or carry out the claimed process. Second, the Examiner must show that the prior art would have provided one of ordinary skill in the art with a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be adequately founded in the prior art and not in an applicant's disclosure. Third, the prior art must teach or suggest all the claim limitations. *In re Vaeck*, 20 U.S.P.Q.2d 1438, 1442 (Fed. Cir. 1991). Fourth, if an obviousness rejection is based on some combination of prior art references, the Examiner must show the suggestion, teaching, or motivation to combine the prior art references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Applicants have amended independent claim 14 to clarify that the enrollment authentication data is stored on the authentication system in substantially randomized data portions. Amended claim 14 now recites in relevant part:

> An authentication system for uniquely identifying a user through secure storage of said user's enrollment authentication data, said authentication system comprising:
>
> a plurality of data storage facilities, wherein each data storage facility ***is remote from said user and*** includes a computer accessible storage medium which stores one of substantially randomized data portions of ~~***at least one piece of enrollment authorization data from***~~ enrollment authentication data; and

(Emphasis added.) Applicants have also amended claim 14 to further clarify that the authentication system which stores the enrollment authentication data is remote from the user. Amended claim 14 now recites in relevant part:

> ...
>
> ***wherein said trust engine comprises an authentication system; and***
>
> ***wherein said trust engine is remote from said user and said user is connected to said trust engine via a communication link.***

(Emphasis added.) Examiner indicates that "Borza discloses storing and processing substantially randomized sensitive data portions." Office Action of April 24, 2006,

page 22. Examiner states that *Borza* relates to constructing a key or key reference from its portions:

> Yet another advantage of encoding the data within an image frame is that the imaging system need only provide data in the form of a portion of an encryption key or a key reference and the biometric data in the form of an image; the computer then processes the image to determine another portion of the key or of the key identifier.

*Borza* at column 6, lines 61-66. However, *Borza* relates to reconstructing a key or key reference from their portions on the user's computer. In contrast, the present invention defines reconstructing the sensitive data from its portions on the trust engine, which is remote from the user.

Examiner also rejected claim 14 because *Epstein* relates to private keys which are "never extant at the user equipment which is not secure." Office Action of April 24, 2006, page 21. This reasoning is both inapposite to the content of claim 14 and is inconsistent with *Epstein*. Claim 14 defines an authentication system which splits, stores, and assembles authentication data, not private keys. Thus, any discussion of private keys in the rejection of claim 14 is irrelevant. Furthermore, even if private keys were relevant to claim 14, in *Epstein* the private keys are stored on the user's smartcard which is attached to the user's machine. See supra pp. 20-21.

*Epstein* relates to comparing user input data to user identifying data in order to authenticate the user. *Epstein* at column 6, lines 12-19. Thus user identifying data is the equivalent of authentication data. *Epstein* relates to storing the user identifying data in its whole form, not in portions. *Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. The user identifying data is previously

> ...loaded in a secure manner during a setup phase when the smartcard [is] issued...with the user's identifying data U derived from information entered by the user.

Id. *Epstein* relates to storing the user identifying data on the user's smartcard.

> **Smartcard also includes a memory for storing** at least the most recently generated random number RN, and the user's private key and **user identifying data**...

*Epstein* at columns 5 and 6, lines 63-67 and lines 1-6. As indicated earlier, the user's smartcard is located in the user's equipment remote from the server. See supra pp. 20-21. Thus, the user identifying data or user authentication data is stored on the

user's equipment, not a remote secure server.

Borza, as explained above, does not cure the deficiencies of *Epstein*. Accordingly, *Epstein*, in further view of *Borza*, does not render the present invention unpatentable. The prior art does not teach or suggest all the claim limitations. Id. Specifically, *Epstein* in view of *Borza* does not teach or suggest to one of ordinary skill in the art storing the authentication data in substantially randomized portions and assembling these portions on the user's machine to form the enrollment authentication data. Consequently, Applicants respectfully request withdrawal reconsideration and the rejection of claim 14 and dependent claims 15-29.

## V. REJECTION OF CLAIMS 56-69 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER PANG (US 6,446,204), AND FURTHER IN VIEW OF BORZA (US 5,995,630)

The Examiner rejected claims 56-69 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,446,204, issued to Pang ("*Pang*"), and in further view of U.S. Patent No. 5,995,630, issued to *Borza*. Office Action of April 24, 2006, page 24. Applicants respectfully traverse.

To maintain a proper rejection under 35 U.S.C. §103, the Examiner must meet four conditions to establish a *prima facie* case of obviousness. First, the Examiner must show that the prior art suggested to those of ordinary skill in the art that they should make the claimed composition or device or carry out the claimed process. Second, the Examiner must show that the prior art would have provided one of ordinary skill in the art with a reasonable expectation of success. Both the suggestion and the reasonable expectation of success must be adequately founded in the prior art and not in an applicant's disclosure. Third, the prior art must teach or suggest all the claim limitations. *In re Vaeck*, 20 U.S.P.Q.2d 1438, 1442 (Fed. Cir. 1991). Fourth, if an obviousness rejection is based on some combination of prior art references, the Examiner must show the suggestion, teaching, or motivation to combine the prior art references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Applicants have amended independent claim 59 to clarify that the enrollment authentication data is stored in substantially randomized portions within multiple data storage facilities. Amended claim 59 now recites in relevant part:

A secure authentication system, comprising:

> a plurality of authentication engines, ***on a remote trust engine,*** wherein ***the data assembling module assembles substantially randomized enrollment authentication data portions, from various data storage facilities, to form the enrollment authentication data***
> ...

(Emphasis added.) This amendment also clarifies that the data assembling module, which is located within the cryptographic system, assembles the substantially randomized data portions to form the enrollment authentication data. The enrollment authentication data is not stored in a "list". Applicants have also amended claim 59 to indicate that a redundancy system uses the authentication results from at least two authentication engines to determine whether the user has been uniquely identified. Amended claim 59 now recites in relevant part:

> a redundancy system which receives said authentication result of at least two of said authentication engines and ***uses said authentication results to*** determine ***[[s] ]*** whether said user has been uniquely identified;
> ...

In contrast, *Pang* relates to a system which,

> includes an authentication server that is connected to multiple dispatchers through [sic] object request broker. Authentication server comprises an authentication engine, an authentication host and a plurality of authentication service providers (simply referred to as providers).

(Emphasis added.) *Pang* at columns 18 and 19, lines 64-67 and lines 1-3. *Pang* relates to an authentication engine which receives authentication requests and then forwards these requests to the appropriate provider. *Pang* at column 19, lines 4-6.

Each provider performs a specific authentication function to restrict access to a particular cartridge. *Pang* at column 20, lines 26-28. *Pang* defines cartridges as, "modules of code for performing specific application or system functions." *Pang* at column 7, lines 9-10. These different providers are used to authenticate users to perform different functions:

> The authenticate( ) [sic] routine validates whether the client requesting the services of the cartridge is authorized to use those services.

*Pang* at column 7, lines 46-47. *Pang* does not teach or suggest using different providers to generate multiple authentication results for the same user request. Thus, *Pang* does not teach or suggest a redundancy system which produces multiple authentication results for the same user request.

*Pang* only provides two examples of the types of providers in the authentication system: BASIC and IP. *Pang* at column 19, lines 54-57. A BASIC provider compares a username and password from the user to a "predefined username/password access list to determine if access should be provided." *Pang* at column 20, lines 32-35. An IP provider compares the user's IP address with an IP access list previously loaded on the provider. *Pang* at column 20, lines 47-50. It is important to note that in both types of providers the user's information is compared to a previously defined list of either usernames and passwords or IP addresses. These lists stored on the providers are thus the equivalent of enrollment authentication data. *Pang* does not teach or suggest storing the lists of user authentication data in substantially randomized portions.

Examiner states that "Borza teaches encryption techniques, biometrics, and storing and processing substantially randomized sensitive data portions to provide security for computer communications and files for computers and networks." Office Action of April 24, 2006, page 25 (emphasis added). The Examiner then quotes from *Borza*:

> Yet another advantage of encoding the data within an image frame is that the imaging system need only provide data in the form of a portion of an encryption key or a key reference and the biometric data in the form of an image; the computer then processes the image to determine another portion of the key or of the key identifier.

*Borza* at column 6, lines 61-66. However, *Borza* relates to reconstructing the keys or key references from their portions on the user's computer. In contrast, the present invention teaches reconstructing the sensitive data from its portions on the trust engine which is remote from the user.

The present invention is not obvious because *Pang* does not teach or suggest storing the equivalent of enrollment authentication data in the form of substantially randomized portions in multiple data storage facilities. Instead, *Pang* discusses storing the equivalent of authentication enrollment data in list form. Borza fails to remedy this deficiency of *Pang*. Also, unlike the present invention which defines generating at least two authentication results to ensure that the authentication system has produced the correct result, *Pang* only discusses producing a single authentication result for each user request. In addition, *Pang* in further view of *Borza* does not render the current invention obviousbecause *Borza* discusses reconstructing a key or

key reference from its parts on the user's computer. In contrast, the present invention defines reconstructing a key or enrollment authentication data on the server remote from the user's computer.

Neither *Pang* nor *Borza*, separately or in combination, teach or suggest storing the authentication data in substantially randomized portions, assembling the enrollment authentication data on a remote server, or using an authentication results from at least two authentication engines to ensure that the system has produced the correct result. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 59 and dependent claims 60-64.

Applicants have amended claim 65 to clarify that the enrollment authentication data is stored in substantially randomized portions within multiple data storage facilities remote from the user. Amended claim 65 now recites in relevant part:

> A trust engine system for facilitating authentication of a user, said trust engine system comprising:
>
> a first trust engine comprising a first depository, ***remote from said user***, wherein said first depository includes a computer accessible storage medium which stores substantially randomized data portions of at least one piece of enrollment authentication data from a plurality of enrollment authentication data ***corresponding to multiple users***;
>
> a second trust engine located at a different geographic location than said first trust engine and comprising:
> ...

(Emphasis added.) Applicants have also amended claim 65 to explain that the authentication data portions are assembled on the data assembling module which is remote from the user. Amended claim 65 now recites in relevant part:

> ...
> wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives authentication data from a user and forwards a request for ***a data assembling module to assemble the*** ~~***said substantially randomized data portions of at least one piece of***~~ said enrollment authentication data ***from substantially randomized data portions*** ~~***to said first and second depositories***~~, and wherein said authentication engine ~~***receives***~~ ***compares*** said authentication data from ***said user*** ~~***said transaction engine***~~ and ~~***said substantially randomized data portions of at least one piece of said***~~ enrollment authentication data ***assembled*** from said first and second depositories, and determines an authentication result***[[.]]***.

***wherein both said first and second trust engines are remote from said user and said user is connected to said trust engines via a communication link.***

(Emphasis added.) As indicated above, *Pang* relates to storing the equivalent of enrollment authentication data in the form of a list. See supra p. 41. *Pang* does not teach or suggest storing authentication data in the substantially randomized data portions in multiple depositories. Id. *Borza* fails to remedy this deficiency in *Pang*. Moreover, *Borza* discusses assembling the keys or key references from their portions on the user's computer.

*Pang* in light of *Borza* does not render the current invention obvious. *Pang* relates to storing enrollment authentication data in whole form at a single location whereas the current invention teaches storing the authentication data in substantially randomized data portions in multiple depositories. Furthermore, *Borza* discusses reconstructing keys or key portions on the user's machine. In contrast, the present invention defines assembling enrollment authentication data in the data assembling module remote from the user.

*Pang* in view of *Borza* does not teach or suggest storing the authentication data in substantially randomized portions or assembling the enrollment authentication data on a remote server as claimed. As a result, the prior art does not teach or suggest all the claim limitations. Consequently, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 65 and dependent claims 66-69.

## CONCLUSION

Applicants have properly stated, traversed, accommodated, or rendered moot each of the Examiner's grounds for rejection. Applicants submit that the present application is now in condition for allowance.

If the Examiner has any questions or believes further discussion will aid examination and advance prosecution of the application, a telephone call to the undersigned is invited. If there are any additional fees due in connection with the filing of this amendment, please charge the fees to undersigned's Deposit Account No. 50-1067. If any extensions or fees are not accounted for, such extension is requested and the associated fee should be charged to our deposit account.

Respectfully submitted,

July 24, 2006

Don J. Pelto
Reg. No. 33,754

Preston Gates Ellis & Rouvelas Meeds LLP
1735 New York Avenue, NW, Suite 500
Washington, DC 20006
Telephone: (202) 661-3710
Facsimile: (202) 331-1024